Department of Homeland Security Daily Open Source Infrastructure Report for 04 April 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports officials conducting a routine inspection of a nuclear reactor at the Turkey Point power plant near Miami found a small hole −− drilled either accidentally or deliberately −− in a pipe that helps maintain pressure. (See item 2)

- The Associated Press reports a C−5 military cargo plane developed problems after takeoff and crashed while attempting to return to Dover Air Force Base on Monday, April 3, breaking apart short of the runway. (See item 12)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *April 03, Associated Press* — **Thousands without power due to storms.** Tens of thousands of Illinoisans remained without power on Monday, April 3, a day after storms packing high winds raked much of the state, killing one man when part of a roof collapsed. About 43,000 homes and businesses in central and southern Illinois had no power Monday, with additional outages in neighboring Missouri affecting about 60,000 customers, Ameren Corp. spokesperson Tim Fox said. That is down from about 270,000 customers who were without power Sunday night in the two states, Ameren said. About 1,100 Ameren workers in Illinois and Missouri scrambled to get the power back on. High winds also knocked out power in Chicago's suburbs to about 6,100

customers of Commonwealth Edison.
Source: http://www.pantagraph.com/articles/2006/04/03/news/doc44314b71704324445164 59.txt

2. *April 02, Associated Press* — **Inspectors find hole drilled in pipe at nuclear power plant.** Officials conducting a routine inspection of a nuclear reactor at the Turkey Point power plant near Miami found a small hole drilled into a pipe that helps maintain pressure, and investigators were trying to determine if the hole was drilled accidentally or deliberately, Florida Power & Light (FPL) officials said Saturday, April 2. The nuclear reactor had been shut down for a routine refueling, FPL spokesperson Rachel Scott said. The 1/8−inch hole was discovered Thursday, March 30, during inspections performed before bringing the unit back online, Scott said. FPL repaired the damaged piping and plans to bring the unit back into service in about a week. The Nuclear Regulatory Commission and FBI are investigating.
Source: http://www.sptimes.com/2006/04/02/State/Inspectors_find_hole_.shtml

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *April 02, Aviation Now* — **Air Force to complete major TSAT risk−reduction efforts.** The U.S. Air Force has a lot riding on the Transformational Satellite (TSAT) project during the coming months. Besides trying to ensure that future combatants have enough secure bandwidth to carry out their missions, the service is attempting to restore its reputation as a space program manager. A series of high−profile cost overruns and schedule delays has badly tarnished the Air Force's "street credentials" in Congress, leading to repeated and deep budget cuts. The stakes are high for the Air Force and industry: billions of dollars in contracts hang in the balance. Congress is receiving a lot of advice on how to "help" the Air Force manage space programs. Some contractors have briefed lawmakers on incremental approaches such as a "TSAT−lite" that would place some future capabilities on platforms already in development. The service has abandoned its original procurement strategy to appease critics and is now pushing for a block approach that would see spacecraft complexity gradually increase. The new plan, devised in part as a response to cuts and criticisms, pushes out the first launch by 18 months to 2014.
Source: http://www.aviationnow.com/avnow/news/channel_space_story.jsp?id=news/040306p1.xml

4. *March 31, Washington Post* — **Favors found in Air Force contracts.** Former Air Force procurement official Darleen A. Druyun, convicted last year for showing favoritism to Boeing Co. while negotiating for a job, also manipulated Pentagon rules to benefit Lockheed Martin Corp. and another defense contractor, according to recent inspector general (IG) reports. The audits, part of an IG review of eight contracts that the Air Force requested last year after Druyun pleaded guilty, found that she helped Lockheed Martin on two airplane contracts

between 1998 and 2001 while serving as a top civilian contracting official. The inspector general focused its criticism on the Air Force, recommending that the service tighten its control of the contracting process. Auditors recommended that the Air Force "sever" that portion of the contract and consider joining with the Marine Corps for a cheaper agreement.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/03/30/AR2006033001970.html

5. *March 31, Air Force Link* — **Air Force finds cost savings for Raptor with multi−year purchasing.** The Air Force believes it can save nearly $500 million by going to multi−year procurement with the next 60 F−22A Raptor aircraft. The Air Force has asked Congress to approve multi−year funding for the remaining 60 Raptors it plans to purchase over the next three fiscal years. Multi−year funding enables the contractor to purchase supplies and parts in quantity and thus at lower prices. By using this approach, the Air Force believes it can realize a five percent savings on the total cost of the remaining aircraft purchases, said Lt. Gen. Donald J. Hoffman, Air Force military deputy for acquisition, during a hearing before the Senate Armed Services Committee subcommittee on air/land. Because the Air Force has reduced the production rate of the Raptor to 20 per year, the cost of each plane will go up. The Air Force believes the savings realized by multi−year procurement will help offset the cost increase from the reduced production rate.
Source: http://www.af.mil/news/story.asp?id=123018297

[Return to top]

Banking and Finance Sector

6. *April 03, Channel Register (UK)* — **UK fights organized crime.** The UK has launched an FBI−style multi−disciplinary agency as part of its plan to fight organized crime. The Serious Organized Crime Agency (SOCA) will tackle drug trafficking, immigration crime, money laundering, and identity fraud by developing intelligence on organized crime and pursuing key suspects while disrupting criminal activity. The agency will bring together more than 4,000 police, customs, and immigration experts to create Britain's first non−police law−enforcement authority. SOCA officers will have wide−ranging powers that are more akin to those held by customs officers rather than the police.
Source: http://www.channelregister.co.uk/2006/04/03/soca/

7. *April 03, New York Times* — **Web's main muggers still out of U.S. reach.** You have probably never met Sergei Kozerev, a former student in St. Petersburg, Russia, but it is possible that he has mugged you. In the online world, he operates under the pseudonym Zo0mer, according to U.S. investigators, and he smugly hawks all manner of stolen consumer information alongside dozens of other peddlers at a Website he helps manage, Forum.TheftServices.com. Tabbot also offers full access to hacked credit union accounts. One, with a $31,000 balance, is being sold for $400. "I can try search specific info such as signature, ssn, dob, email access," Tabbot writes. The online trade in stolen financial data is thriving. In the transnational, Internet−driven market for stolen financial and consumer data, some thieves are easier to nab than others. And where Russians and East Europeans like Zo0mer have become the leaders in the stolen data trade, the English−speakers, particularly Americans, are the easiest to catch.
Source: http://www.iht.com/articles/2006/04/02/business/data.php

8. *April 02, Associated Press* — **New study finds fewer victims of identity theft.** An estimated 3.6 million U.S. households reported being victims of identity theft, according to a government study that counted misuse of someone else's cell phone, credit card or personal information. The figures released by the Department of Justice (DOJ) differ from findings of a previous Federal Trade Commission (FTC) study that estimated 9.3 million victims of the crime for the same period. The department said the most frequent victims of identity theft were households headed by people age 18 to 24; those in urban or suburban areas; and those with incomes of at least $75,000. Of the 3.6 million victimized households, the study said an estimated 1.7 million discovered unauthorized use of credit cards during the six−month period; about 900,000 households experienced theft from other types of existing accounts. An earlier report by the FTC estimated about 10.1 million people experienced identity theft in 2003 and 9.3 million in 2004. The DOJ said the different results may be due to differences in the methods used to collect the data, the period of time considered, and counting methods.
Report: http://www.ojp.usdoj.gov/bjs/abstract/it04.htm
Source: http://www.chron.com/disp/story.mpl/front/3765229.html

9. *March 31, CNET News* — **Phishers set hidden traps on eBay.** Click on an eBay auction listing, and you could get an unwanted result: a fake eBay login page, created by scammers looking to pilfer your username and password. With about 181 million users worldwide, eBay is arguably the world's most popular online marketplace. As such, the company, with its online payment unit PayPal, is among the biggest targets for online scammers −− including phishers. Cyber crooks typically use spam e−mail to lure people to their Web traps. But on eBay, they also take advantage of the auction listings on the site itself. Some of the scams run on the auction Website are almost invisible to the untrained eye. eBay lets sellers customize their auction pages using Web programming techniques and automated tools. However, attackers are abusing this freedom to build auction pages that include a rigged listing. When potential customers click on the link, it sends them to a phishing site. eBay is aware of such abuse of its service for trickery by cyber crooks, Catherine England, an eBay spokesperson, said.
Source: http://news.zdnet.com/2100−1009_22−6056687.html

[Return to top]

Transportation and Border Security Sector

10. *April 03, Associated Press* — **Truck carrying explosives crashes in Utah.** A semitrailer carrying a potentially dangerous blend of explosive materials crashed in Uintah County on Thursday, March 30, forcing the evacuation of two nearby homes. No injuries were reported, the Utah Highway Patrol (UHP) said. The truck rolled over on Utah 88 near Pelican Lake and the town of Ouray, about 175 miles east of Salt Lake City. The truck was carrying 40,000 pounds of ammonium nitrate, 10,000 blasting caps and several hundred pounds of dynamite, UHP spokesperson Jeff Nigbur said. "Ammonium nitrate is a fairly stable substance, but when you put it in contact with an ignition source, like blasting caps, it could possibly turn into a dangerous situation," Nigbur said. Nigbur did not know how the materials were packaged, but said he didn't believe they could get mixed together. Authorities evacuated homes within a two−mile radius around the crash.
Source: http://www.casperstartribune.net/articles/2006/04/03/news/re

gional/5b73f3563ae61a4c872571420075c165.txt

11. *April 03, Associated Press* — **Mexican authorities shut down Aerocalifornia for lack of security.** Mexico's federal Civil Aviation Department has suspended operations at Aerocalifornia after determining that the low−cost carrier failed to meet adequate safety standards, Mexican news media reported Monday, April 3. The suspension follows inspections by federal authorities beginning more than a year ago, when the airline was instructed to make changes to improve operations. One of the inspections showed that the airline had one−third of its fleet grounded and was taking parts from the decommissioned airplanes to keep others operating, the department said.
Source: http://www.azcentral.com/news/articles/0403MexicoAirline03−O N.html

12. *April 03, Associated Press* — **C−5 cargo plane crashes at Dover Air Base.** A huge military cargo plane developed problems after takeoff and crashed attempting to return to Dover Air Force Base on Monday, April 3, breaking apart short of the runway, officials said. All 17 people aboard survived, though several were injured. The C−5 Galaxy, the military's largest plane, broke in two just behind the cockpit, leaving the cockpit at a right angle to the fuselage. The tail assembly ended up several hundred yards from the plane, and one of the engines was thrown forward by the impact, but there was no evidence of fire. The C−5 was being flown by a reserve crew from the 512th Airlift Wing, said Captain John Sheets of the Air Mobility Command at Scott Air Force Base in Illinois. According to initial reports, the plane had just taken off and had some indications of a problem, said Col. Ellen Haddock, spokesperson at the Pentagon's Joint Chiefs of Staff. It turned back to land and fell short of the runway, she said. It wasn't immediately clear if the plane was carrying cargo when it went down.
Source: http://www.forbes.com/technology/feeds/ap/2006/04/03/ap26423 65.html

13. *April 02, USA TODAY* — **Cases of unruly airline passengers fall, but bad behavior still rampant.** Reports of disruptive and unruly passengers have remained high since the September 11, 2001, attacks, according to government data. Airlines and federal regulators, armed with a slew of new security precautions, have warned that misbehaving passengers face tough penalties. But that hasn't led to a significant decrease in incidents. There were 349 cases of unruly passengers reported to federal aviation agencies last year, the second highest total in the past decade. The highest yearly total during that period was a large spike of 482 cases in 2004; it's unclear why such an increase occurred that year. Both the Federal Aviation Administration (FAA) and the Transportation Security Administration (TSA) handle many of the most serious incidents, which range from passengers refusing to take their seats to assaults of crewmembers. The number of cases reported to aviation agencies was below 200 per year in the mid−1990s. The number of cases reached 299 in 2001, the year that terrorist hijackings prompted a revamp of security rules and a change in how flight crews react to misbehavior. Both the FAA and TSA say it's unclear why the numbers remain high.
Source: http://www.usatoday.com/travel/news/2006−04−02−unruly−passen gers_x.htm?POE=NEWISVA

14. *March 31, CNET News* — **Singapore unveils biometric passport.** Starting in August, all passport holders in Singapore can apply for new travel documents with additional security features designed for international standards. The biometric passport, called BioPass, was unveiled Friday, March 31, by the government. Each e−passport contains a polycarbonate page

that is embedded with a contactless chip, carrying the owner's facial and fingerprint biometric identifiers. According to Singapore's Immigration and CheckPoints Authority, the BioPass carries enhanced security features, such as multiple laser images, that are difficult to tamper with. Wong Kan Seng, Singapore's Minister for Home Affairs, noted that the BioPass has achieved Level II certification under the United States' Visa Waiver Program, which requires participating countries to issue e−passports by October 26 of this year. "This means that tests conducted by the U.S. Department of Homeland Security have shown the BioPass to be in full compatibility with its passport readers," he said. Singapore, along with Australia, New Zealand, and the U.S., has been involved in an International Live Test since January. These trials are expected to be completed by April 15.
Source: http://news.com.com/Singapore+unveils+biometric+passport/2100−1029_3−6056746.html?tag=cd.top

15. *March 31, Computerworld* — **IT upgrades slow BART trains in San Francisco.**
Unsuccessful software upgrades made to San Francisco’s Bay Area Rapid Transit (BART) train system last Sunday, March 26 stranded thousands of commuters for up to two hours Monday and Tuesday when the trains had to be stopped for safety reasons while the IT system was repaired. Linton Johnson, a BART spokesperson, said the delays and shutdowns occurred after IT staffers did maintenance upgrades to the software that coordinates and runs the trains, tracks, operating signals, and track switches. The attempted upgrades caused the system to crash twice during the following 48 hours, he said. On Monday and Tuesday, the crashes caused transit delays when the trains were halted so they didn’t run into each other, he said. After those software problems, BART IT workers on Wednesday decided to install backup software for redundancy in case of continuing problems. “We were rushing to do the right thing...However, in the process of installing that backup system, we interfered with a [network switch] that crashed our system,” Johnson said. Normally, such maintenance is avoided during the week, he said. The backup system installation was done on Wednesday to try to stop the problems experienced earlier in the week.
Source: http://www.computerworld.com/softwaretopics/software/story/0,10801,110107,00.html

[Return to top]

Postal and Shipping Sector

16. *April 03, Associated Press* — **New Orleans postmark returns for first time since Katrina.**
For the first time since Hurricane Katrina, the Postal Service began processing mail Monday, April 3, in New Orleans, LA, a move officials say should eliminate delivery times of a week or more for cross−town mail. “Our expectation is that we will get back to 95 percent overnight service,” New Orleans Postmaster Alan Cousins said. An embargo continues for magazines, newspapers, catalogs and other second−class mail, though it likely will be lifted next month, officials said. The processing and distribution center is housed in the same building as the main New Orleans post office. It closed after Katrina's floodwaters destroyed the electrical equipment. Before the storm, the plant processed six million to eight million pieces of mail a day for the New Orleans area, as well as for parts of Mississippi and Alabama.
Source: http://www.signonsandiego.com/news/nation/katrina/20060403−0638−katrina−mail.html

17. *April 03, Rocky Mountain Telegram (NC)* — **Drill to test biohazard preparedness at post office.** A fake anthrax scare will hit the Rocky Mount, NC, Post Office Wednesday, April 5. Police, fire and state health officials will set up at the post office to simulate the detection of anthrax at the post office. Area and state decontamination teams will respond to the planned call. When the alarm is sounded, the post office will be evacuated and the participants inside will be taken to a decontamination area.
Source: http://www.rockymounttelegram.com/news/content/news/stories/ 2006/04/03/drill.html

[Return to top]

Agriculture Sector

18. *April 03, Wisconsin Ag Connection* — **Pig mortality from PCV−2 virus bears watching.** A recent increase in mortality in growing and finishing pigs associated with porcine circovirus type 2 (PCV−2) infections has prompted veterinarians to urge pork producers to be on the alert for the possibility in their own herds. Peter Bahnson, a swine veterinarian at the University of Wisconsin−Madison School of Veterinary Medicine, says that until recently, PCV−2 was associated primarily with nursery mortality. The syndrome, often referred to as PMWS, or Postweaning Multisystemic Wasting Syndrome, has appeared sporadically in the U.S. The syndrome was first reported in the prairie provinces of Canada in the 1990s and then spread to Europe. In the past 12−18 months, however, mortality attributed to PCV−2 has been reported in older pigs in Canada, especially those 10−15 weeks of age, and primarily in Quebec and Ontario. Veterinarians attending the recent American Association of Swine Veterinarian's annual meeting in Kansas City, MO, reported seeing a similar syndrome of elevated grow/finish mortality in some U.S. herds.
PCV−2 information: http://www.addl.purdue.edu/newsletters/2005/Fall/pcv2.htm
Source: http://www.wisconsinagconnection.com/story−state.cfm?Id=401& yr=2006

19. *April 03, Economic Research Service* — **Value of plant disease early−warning systems.** Early−warning systems for plant diseases are valuable when the systems provide timely forecasts that farmers can use to inform their pest management decisions. To evaluate the value of the systems, this study examines, as a case study, the U.S. Department of Agriculture's coordinated framework for soybean rust surveillance, reporting, prediction, and management, which was developed before the 2005 growing season. The framework's linchpin is a Website that provides real−time, county−level information on the spread of the disease. The study assesses the value of the information tool to farmers and factors that influence that value. The information's value depends most heavily on farmers' perceptions of the forecast's accuracy. The study finds that the framework's information is valuable to farmers even in a year with a low rust infection like that of 2005. It is estimated that the information provided by the framework increased U.S. soybean producers' profits by a total of $11−$299 million in 2005, or between 16 cents and $4.12 per acre, depending on the quality of information and other factors. The reported cost of the framework was between $2.6 million and almost five million dollars in 2005.
A Case Study of USDA's Soybean Rust Coordinated Framework:
http://www.ers.usda.gov/publications/err18/err18.pdf
Source: http://www.ers.usda.gov/publications/err18/

[Return to top]

Food Sector

20. *April 03, Animal and Plant Health Inspection Service* — **Electronic system to ease import process implemented.** As part of the U.S. Department of Agriculture's (USDA) overall eGovernment initiative to transform and enhance the delivery of its programs, services and information, USDA's Animal and Plant Health Inspection Service Monday, April 3, launched ePermits, a new electronic system to streamline the import process. The new system, which is being released in multiple phases, is a Web−based tool that allows the electronic filing, processing and tracking of permit applications. The current phase allows individuals to process permit applications on−line for certain plant protection and quarantine and biotechnology and regulatory services' notifications. Veterinary services is in the process of finalizing its system and plans to launch its ePermits section on July 3. More advances are underway including the ability to apply for more types of APHIS permits and a feature that will allow APHIS officials to generate and print shipment labels with barcodes. Once the barcode is scanned, it will immediately verify that the permit is valid.
Source: http://www.aphis.usda.gov/newsroom/content/2006/04/epsystem. shtml

21. *March 31, U.S. Food and Drug Administration* — **Chocolate products recalled.** Dagoba Organic Chocolate of Ashland, OR, is recalling their "ECLIPSE 87%," "LOS RIOS 68%," and "PRIMA MATERA 100%" dark chocolate products in retail and bulk formats because they contain high levels of lead. The products were distributed nationally through wholesale food distributors and through stores that sell organic, natural and/or specialty foods, as well as via select Internet sites. No documented illnesses associated with these products have been reported to date. The recall was the result of a routine sampling program by the company which revealed that the finished products contained high levels of lead. The company has ceased the production and distribution of the product.
Source: http://www.fda.gov/oc/po/firmrecalls/dagoba03_06.html

[Return to top]

Water Sector

22. *April 02, Star Bulletin (HI)* — **More sewage pours into Oahu waters.** Officials are expected to keep surfers and swimmers out of waters off Ala Moana Bowls and Magic Island again Sunday, April 2, after another sewage spill Friday, March 31, sent more bacteria into the water. On Friday, there were nine large sewage spills island−wide and several smaller spills as manholes overflowed. On Friday, about 1.8 million gallons of sewage spilled when a power outage shut down the Ala Moana Pump Station, which was working at maximum capacity because of the recent heavy rains. An additional 6,900 gallons of sewage overflowed from manholes at Ala Moana Boulevard and Atkinson Boulevard. Signs had already been posted at beaches in the area after more than 40 million gallons of untreated sewage went into the Ala Wai Canal after a main break last week.
Source: http://starbulletin.com/2006/04/02/news/story06.html

23. *April 01, Washington Post* — **Environmental Protection Agency may weaken rule on water quality.** The U.S. Environmental Protection Agency (EPA) is proposing to allow higher levels of contaminants such as arsenic in the drinking water used by small rural communities, in response to complaints that they cannot afford to comply with recently imposed limits. The proposal would roll back a rule that went into effect earlier this year and make it permissible for water systems serving 10,000 or fewer residents to have three times the level of contaminants allowed under that regulation. About 50 million people live in communities that would be affected by the proposed change. In the case of arsenic, the most recent EPA data suggest as many as 10 million Americans are drinking water that does not meet the new federal standards. Benjamin Grumbles, assistant administrator for EPA's Office of Water, said the agency was trying to satisfy Congress, which instructed EPA in 1996 to take into account that it costs small rural towns proportionately more to meet federal drinking water standards. Under the Safe Drinking Water Act Amendments of 1996, complying with federal drinking water standards is not supposed to cost water systems more than 2.5 percent of the median U.S. household income.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/03/31/AR2006033101629.html

[Return to top]

Public Health Sector

24. *April 03, Associated Press* — **Doctors report rise in flesh−eating bacteria.** Some doctors in Kentucky say they are seeing a rise in the number of cases of flesh−eating bacteria, a rare disease that is potentially lethal. One germ to blame for the illness is a resistant staph bacteria −− a growing threat fueled by the overuse of antibiotics. Also on the rise are serious problems linked to Group A strep, the bacteria that causes many other cases of flesh−eating disease. Kentucky reported 62 cases of invasive disease caused by this germ in 2004, up from 39 in 2001.
Source: http://news.cincinnati.com/apps/pbcs.dll/article?AID=/20060403/NEWS0103/604030347/−1/CINCI

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

25. *April 03, Federal Computer Week* — **Short Message Service earns valued role as a link of last resort for crisis communications.** When disaster strikes, Short Message Service (SMS) has a major advantage over cellular voice calls and wireless e−mail devices. Text messages do not rely on voice channels for transmission, and they don’t piggyback on enterprise e−mail

servers. Instead, SMS messages travel as small packets of data on a wireless carrier's control channel, the same portion of the spectrum that keeps a cellular network comprised of a particular phone's location and status. Because SMS messages are isolated in the control channel and are often unfazed by heavy traffic or adverse conditions that can overwhelm wireless networks, text messages can get through when most other methods of communication fail. Hence, some government officials are beginning to build SMS use into disaster planning exercises. Michigan's use of SMS is blended with extensive reliance on an enterprise−wide communication software platform designed to blast notifications to frontline responders and enable two−way communication through the State Emergency Operations Center.
Source: http://www.fcw.com/article92790−04−03−06−Print

26. *April 02, Daily Progress* — **Virginia county is one step closer to interoperable communications.** Emergency communications officials in Albemarle County, VA, have the area's long−awaited new radio system up and running Sunday, April 2, in what they say is the first step toward allowing local fire, rescue and police agencies to talk with each other during emergencies. The 800−megahertz system will give agencies the ability to communicate directly with one another, something they currently cannot do, said Lee Catlin, spokesperson for Albemarle County. Police, fire and rescue each have a separate system, which makes it difficult, if not impossible, to communicate with each other directly during emergencies, Catlin said. The primary benefit of the new 800−megahertz system is the ability to put all responders on the same frequencies. It is expected to provide better coverage for the county's hill−and−dale geography and make radio communications possible in areas that the current system's walkie−talkies cannot reach.
Source: http://www.dailyprogress.com/servlet/Satellite?pagename=CDP%2FMGArticle%2FCDP_BasicArticle&c=MGArticle&cid=1137835100616 &path=!news

27. *April 01, South Bend Tribune (IN)* — **Indiana public works staff prepare for potential terrorist attacks.** Last week, Michiana, IN, hosted an intense, three−day terrorism preparedness training course for public works and safety personnel. Instructors from the National Emergency Response and Rescue Training Center, based out of Texas A & M University, trained local officials on maintaining public safety and protecting infrastructure in the case of a terrorist incident. Although police and fire are the first responders, explained John Wiltrout, director of treatment for South Bend Waterworks, public works agencies are key players in the aftermath. This is the first time public works has had terrorism preparedness training.
Source: http://www.southbendtribune.com/apps/pbcs.dll/article?AID=/20060401/News01/604010369/CAT=News01

28. *March 30, Radio Iowa* — **Iowa conducts emergency exercise.** The Iowa Department of Public Health launched an emergency preparedness exercise, Operation Viper, Thursday, March 30, that involved six counties' response to a mock infectious disease outbreak. The evaluation of this exercise will be used to identify gaps in emergency plans and make improvements.
Source: http://www.radioiowa.com/gestalt/go.cfm?objectid=F0E491AD−D76A−4906−8CF6C5A65A1382D5

[Return to top]

Information Technology and Telecommunications Sector

29. *April 03, IDG News Service* — **Trend Micro data revealed due to virus.** The failure of a Trend Micro Inc. employee to install his company's own antivirus software led to the uploading of some company reports to a popular Japanese peer−to−peer file−sharing network, the company said Monday, April 3. In disclosing the data leak, Trend Micro became the latest of a number of corporations or government agencies to report data losses as a result of viruses on the Winny network. Winny can be downloaded at no charge and is a popular way for Japanese Internet users to exchange music and video files.
Source: http://www.computerworld.com/securitytopics/security/holes/story/0,10801,110142,00.html

30. *April 03, Washington Post* — **Alcatel agrees to buy Lucent; Merger subject to anti−trust, national security review.** France's Alcatel Sunday, April 2, said it agreed to acquire Lucent Technologies Inc. for about $13.4 billion in stock in a deal analysts said would create the largest equipment supplier to telephone and wireless carriers around the world. The companies, which held abortive merger talks five years ago, said the combination would give them a stronger range of products, a greater ability to compete as their customers consolidate into fewer big players and a geographic reach almost evenly balanced among the Americas, Europe and the rest of the world. The companies said they would take steps to ensure that sensitive work carried out for the U.S. government by Lucent and its vaunted Bell Labs research arm would be overseen by an independent U.S. subsidiary with three U.S. citizens as its directors. The merger must be cleared by European Union and American antitrust authorities, as well as the interagency Committee on Foreign Investments in the United States, which scrutinizes foreign purchases of U.S. companies to ensure they do not threaten national security.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/04/02/AR2006040200867.html

31. *March 30, Secunia* — **McAfee VirusScan DUNZIP32.dll buffer overflow vulnerability.** A vulnerability has been discovered in McAfee VirusScan, which potentially can be exploited to compromise a user's system. Analysis: The vulnerability is caused due to a boundary error in a 3rd−party compression library (DUNZIP32.dll) when processing virus definition files. This can be exploited to cause a buffer overflow via a specially crafted definition file. Affected software: McAfee SecurityCenter 6.x; McAfee VirusScan 10.x. Solution: Update to the fixed version of DUNZIP32.dll via online update.
Source: http://secunia.com/advisories/19451/

32. *March 30, IT Observer* — **Report on targeted attacks on corporate networks released.** Panda Software has released a white paper entitled, "Protection for Corporate Networks Against Targeted Attacks," to offer network administrators information about this type of threat and how to combat it.
This paper can be freely downloaded from (registration required):
http://www.pandasoftware.com/download/register.asp?CodigoProducto=23&TipoLead=2&TipoUsuario=2&Tipo=5&Ref=WW−EN−NOATTACK−603&Idioma=2&Country=US&sec=down&docId=R04&track=
Source: http://www.it−observer.com/news/5979/report_targeted_attacks__corporate_networks/

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a vulnerability in the way Microsoft Internet Explorer handles the createTextRange() DHTML method. At least 4 exploits are in the public domain.

VU#876678 − Microsoft Internet Explorer createTextRange() vulnerability
http://www.kb.cert.org/vuls/id/876678

Known attack vectors for this vulnerability require Active Scripting to be enabled in Internet Explorer. Disabling Active Scripting will reduce the chances of exploitation. Until an update, patch or more information becomes available, US−CERT recommends disabling Active Scripting as specified in the Securing Your Web Browser document.
http://www.us−cert.gov/reading_room/securing_browser/#how_to__secure

We will continue to update current activity as more information becomes available.

Phishing Scams
US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. Specifically, sites that provide online benefits are being targeted. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 25 (smtp), 41170 (−−−), 42011 (−−−), 15000 (hydap), 49200 (−−−), 55620 (−−−), 139 (netbios−ssn) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.